

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of)	
)	
Implementation of the Telecommunications)	
Act of 1996: Telecommunications Carriers')	CC Docket No. 96-115
Use of Customer Proprietary Network)	
Information and Other Customer)	
Information)	

REPLY COMMENTS OF VERIZON WIRELESS

Commenters representing a broad cross-section of the wireless ecosystem recognize that the diverse array of players with access to information stored on mobile devices in today's open Internet environment requires a comprehensive approach to protecting consumer privacy. The record reflects broad support for a technology- and competitively-neutral privacy framework applicable to all players, and affirms that the Commission cannot achieve that objective through regulatory mandates on wireless service providers. Parties supportive of such mandates fail to acknowledge the array of parties that can access customer data on mobile devices, service providers' limited technical ability to prevent access to such data, and the limited scope of the Commission's statutory authority. Moreover, several inaccurately describe wireless service providers' privacy practices.

The comments thus do not support the imposition of new regulations on wireless service providers, but instead underscore the need for a comprehensive privacy framework that will apply to all parties that can access consumer information on mobile devices. Developing such a framework requires a realistic and holistic assessment of consumer privacy needs and expectations as well as a reasoned code of conduct that will apply to all stakeholders accessing

consumer data in today's complex Internet environment. NTIA's multi-stakeholder process remains an appropriate venue for developing such a framework.¹

I. CONSUMERS NEED A COMPREHENSIVE APPROACH TO PRIVACY THAT INCLUDES WIDELY-APPLICABLE CODES OF CONDUCT

A. The Record Reflects Broad Support for Addressing Mobile Device Privacy Issues Consistently Across the Internet Ecosystem

Verizon Wireless and other commenters demonstrated that many players other than wireless service providers have access to information stored on mobile devices in today's open Internet environment, and that wireless service providers are not technically capable of restricting access to all customer data stored on devices.² Commenters further underscored that the Commission has only limited jurisdiction in this area, and that consumers would not enjoy the privacy protection they deserve if the agency were to exercise that limited authority.³ The record thus demonstrates that, in order to more effectively protect consumer privacy, the Commission should instead allow and encourage the development of a competitively- and technology-neutral privacy framework that applies to all players equally.⁴

¹ See NTIA/U.S Dept. of Commerce, *Multistakeholder Process To Develop Consumer Data Privacy Code of Conduct Concerning Mobile Application Transparency*, 77 Fed. Reg. 38597 (June 28, 2012).

² See Verizon Wireless Comments at 2-5; AT&T Comments at 6-7; Consumer Electronics Ass'n ("CEA") Comments at 3-4; CTIA Comments at 4; Future of Privacy Forum Comments at 4-6; TechAmerica at 3-4; Center for Democracy and Technology ("CDT") Comments at 7-8; *see also* Federal Trade Commission ("FTC") Comments at 4 (discussing actions against Facebook, Google and MySpace).

³ See Verizon Wireless Comments at 5-8; AT&T Comments at 8-9, 21-22; CEA Comments at 4-9; CDT Comments at 3-8; CTIA Comments at 3-10; Sprint Comments at 11-14; *see also* FTC Comments at 1 (citing its "jurisdiction over the activities of all of these entities [within the mobile ecosystem], other than the common carrier activities of telecommunications carriers").

⁴ See Verizon Wireless Comments at 2, 6-7; AT&T Comments at 10-13; CDT Comments at 8; Information Technology and Innovation Foundation Comments at 4; TechAmerica Comments at 4.

Commenters advocating new regulations, in contrast, fail to acknowledge the limits of the Commission's authority under Section 222 of the Communications Act. Others presume a degree of service provider intervention in other players' business activities that does not exist in the open Internet environment. Indeed, such regulations could not prove effective absent a fundamental restructuring of Internet technology and the ecosystem that has developed around it.

Valid concerns exist about consumer privacy in today's complex open Internet environment. The importance of clear and adequate disclosures to consumers concerning the type and use of data collected,⁵ the fact that different types and uses of information may warrant different safeguards,⁶ and the need for adequate safeguards to protect teens and children,⁷ are all appropriate considerations in determining how best to protect customer privacy through a comprehensive framework that applies equally to all players. As discussed below and in Verizon Wireless' comments, however, a venue such as NTIA's multi-stakeholder process, which includes all of the relevant players, rather than the Commission's exercise of authority under Section 222 of the Act, will best achieve this objective.

B. Commenters Advocating New Regulations Fail to Acknowledge Service Providers' Lack of Control Over the Open Internet and Limits on the Commission's Authority

The Commission has already exercised the scope of its Section 222 authority to impose meaningful notice and consent, security, breach notification, and other safeguards on the use of

⁵ See Common Sense Media Comments at 2; Comments of Greek Orthodox Archdiocese of America, United Church of Christ Office of OC, Inc., and US Conference of Catholic Bishops at 4-5.

⁶ See Electronic Privacy Information Center ("EPIC") Comments at 11.

⁷ See Common Sense Media Comments at 3.

CPNI, so further regulations in this area, as some commenters propose, are unnecessary.⁸

Further, many of those proposed regulations are premised on the mistaken assumption that service providers can now dictate the capabilities of device components and third party apps.

For example, even as it concedes that the Commission is subject to jurisdictional limits, the Center for Digital Democracy posits “that there is a relationship between the carriers and the mobile marketing service platforms” and that the agency should “identify mobile screen design and data collection practices that are unfair and deceptive to consumers, and propose appropriate new safeguards.”⁹ Such regulation would be well outside Section 222’s parameters. Common Sense Media proposes a number of new regulations concerning disclosure, opt-in, and breach notification, on the basis that the carrier’s role in the “interconnected eco-system” leaves it best positioned to protect consumer privacy, even with respect to the acts of third parties.¹⁰ Verizon Wireless already notifies customers how it uses customer information and provides customer choice to the appropriate degree and, as noted above, the Commission already imposes breach notification requirements for CPNI.¹¹ There is no basis for additional regulation. Verizon Wireless and other commenters demonstrate that carriers cannot effectively protect consumer privacy on a holistic basis in today’s Internet marketplace.¹²

⁸ See Common Sense Media Comments at 2; Electronic Frontier Foundation (“EFF”) Comments at 2-3; EPIC Comments at 10-16; Comments of New American Foundation, Benton Foundation, Center for Media Justice, Chicago Media Action, Free Press, Institute for Local Self-Reliance, Media Alliance, Peoples Production House, Public Knowledge, and the Peoples Channel & Durham Community Media at 8-12.

⁹ Center for Digital Democracy (“CDD”) Comments at 2, 6.

¹⁰ See *id.* at 3-4.

¹¹ See 47 C.F.R. § 64.2011. Breach notification requirements exist for cable and satellite video services, and many states impose such requirements as well.

¹² See *supra* notes 2-3.

Finally, the New America Foundation and associated parties (“NAF”) proffer a breathtakingly expansive view of the Commission’s authority, asserting that, for example, “texting and data logs” are “subject to Section 222(c) ... because they pertain to a telecom service insofar as (1) texting and data are part of the same billing package as voice, used on the same device, advertised and marketed as part of the same service, and (2) they use the consumer’s phone number.”¹³ Under this interpretation, as a practical matter many information services would become subject to Section 222(c) simply by virtue of being offered by a service provider – an approach the Commission rejected years ago, finding that information derived from information services is not covered because “Section 222(c)(1) prohibits the use of CPNI *only where it is derived from the provision of a telecommunications service ...*”¹⁴ While the “cellular landscape” may have changed since 2007,¹⁵ the scope of the Commission’s statutory authority has not changed and, indeed, NAF would have the Commission act where the FTC claims jurisdiction.¹⁶

C. A Privacy Framework that Accounts for the Sensitivity and Proposed Use of Data, Not Prescriptive Regulations, Will Best Protect Consumer Privacy

Verizon Wireless and other parties illustrated that the different types of data available to different entities, and the range of potential consumer-beneficial uses of that data, warrant a flexible approach that applies to all players.¹⁷ Several commenters, however, propose

¹³ See NAF Comments at 2 and n.7.

¹⁴ See Verizon Wireless Comments at 8 n.9 (citing *Implementation of the Telecommunications Act of 1996; Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, ¶ 158 (1999) (emphasis added)).

¹⁵ See NAF Comments at 3.

¹⁶ See FTC Comments at 1.

¹⁷ See Verizon Wireless Comments at 8-9.

regulations that would apply only to service providers and are not calibrated to the sensitivity and intended use of the particular data collected. Categorically subjecting the use or sharing of handset data to opt-in consent,¹⁸ for example, would preclude a service provider from using the data for purposes necessary to provide the service in question, or that fall within the subscriber's service expectations such as data that detects device abnormalities.¹⁹ Similarly, EPIC's proposal to "[r]equir[e] service providers to provide reasonable access to personal data stored about them, as well as an easily navigable mechanism" for correction and removal,²⁰ is not only unrelated to mobile devices, but is not reflective of the sensitivity of the information and could result in development of elaborate data access mechanisms that are largely unutilized. Further, *all* ecosystem players should consider providing appropriately tailored data access mechanisms, so this issue is also more appropriate for venues such as NTIA's multi-stakeholder process.

EPIC also baldly asserts that "because mobile carriers bear no legal responsibility for the downstream uses of consumer data, they have few incentives to ensure that third parties respect the context in which consumers agreed to the collection of their data," and further suggests that Verizon Wireless in particular does not "incorporate[] respect for context" with respect to sharing data with third parties.²¹ This is not true. In fact, maintaining customers' trust and satisfaction is a significant incentive to provide appropriate privacy protections, as consumers who fear their data is not being adequately protected will not use our services and may choose

¹⁸ See Common Sense Media Comments at 2; EPIC Comments at 12; NAF et al. Comments at 9.

¹⁹ See Verizon Wireless Comments at 9 (access to device data "such as an abnormal rate of device reboot or crash, abnormally low battery life or memory, or abnormal amount of time spent in a particular radio air interface or without a wireless connection, can be critical to assisting a customer with device problems").

²⁰ See EPIC Comments at 13-14.

²¹ See *id.* at 10-11.

another provider. Further, “respect for context” permeates Verizon Wireless’ privacy practices. In some instances it may be necessary to share customer information with third party vendors in order to provide service – a use that clearly falls within a customer’s expectations. Sharing information with third parties in order to deliver a service the consumer has requested is precisely what the “Respect for Context” principle recognizes: “Companies should limit use and disclosure of personal data to purposes that are consistent with both the relationship that they have with consumers and the context in which consumers originally disclosed the data, and where use or disclosure occurs for other purposes, consumers should receive heightened transparency and choice concerning those uses.”²² These facts, together with other information in the record, indicate that service providers have significant incentives to protect sensitive consumer data.²³

II. COMMENTERS’ INACCURATE DESCRIPTIONS OF VERIZON WIRELESS PRACTICES ARE RED HERRINGS THAT PROVIDE NO BASIS FOR REGULATION OF SERVICE PROVIDERS

Some commenters make unsupported assertions about carrier practices, including Verizon Wireless practices, as a purported basis for new regulations. Most of the practices appear unrelated to data stored on mobile devices and, with respect to Verizon Wireless at least, the descriptions are inaccurate or incomplete at best. As such, they provide no basis for Commission regulation in this area.

CDD, for example, asserts without explanation that Verizon enables “‘email captures’ and other data collection,” citing to a URL that describes a Verizon Enterprise Services (not

²² See The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf> (February 2012) at 15.

²³ See AT&T Comments at 14-24; Sprint Nextel Comments at 3-5, 7-11.

Verizon Wireless) digital media transmission offerings for video content providers.²⁴ These offerings are current or future enterprise products aimed at large businesses – not end user consumer offerings. These products are subject to review for consistency with Verizon corporate privacy policies as a matter of course, like any other service Verizon offers. Further, the products do not entail any sort of “email capture.”

EFF references a program that Verizon Wireless publicly announced last fall to use and share *aggregated* data. The program discloses nothing about an individual customer, cannot be reverse-engineered to obtain information about a specific customer, and has a robust notice and opt-out process. Verizon Wireless already explained the program in considerable detail to policymakers and in notices to subscribers before the program was implemented, so the Commission should dismiss EFF’s glib assertion that Verizon Wireless “finally got around to sending a polite email to customers” about the program.²⁵ EFF also asserts, without any support, that app platform and operating system vendors’ ability to deploy security fixes to handsets is “fundamentally limited by carrier intransigence.”²⁶ EFF’s statement reveals a fundamental misunderstanding of carrier practices. In fact, given today’s competitive wireless market Verizon Wireless is highly incented to implement security updates that protect its subscribers and its network, and has streamlined its processes to make updates available to subscribers via a seamless over-the-air (OTA) process as soon as practicable. Doing so, however, requires

²⁴ CDD Comments at 12.

²⁵ EFF Comments at 2. Verizon Wireless briefed prominent legislators about the program and, while some preferred an “opt-in” approach, they commended Verizon Wireless’ “efforts to be transparent with [its] customers” and noted that the company “followed the law and exceeded common industry practices in this area.” See <http://markey.house.gov/press-release/nov-4-2011-verizon-responds-questions-about-privacy-targeted-advertising-practices>.

²⁶ EFF Comments at 7.

cooperation and testing with app platforms, OS vendors, and the OEMs, in a nontrivial process that can take at least several weeks from start to finish.

EPIC also makes blanket assertions that carriers “share data with third parties for use in behavioral advertising.”²⁷ As a threshold matter, this is unrelated to Verizon Wireless’ practices for devices and, in any event, online behavioral advertising does not compromise customers’ privacy interests when companies provide notice and the ability for the customer to choose whether to permit behavioral advertising.²⁸ Citing to Verizon Wireless’ privacy policy, EPIC also misleadingly asserts that “Verizon requires consumers to forgo services if [its subscribers] want to prevent the collection of their data.”²⁹ In fact, Verizon Wireless’ privacy policy simply reflects that data collection may be necessary to provide and maintain the very service to which the customer has subscribed, and to protect the security of the device and the network;³⁰ enabling subscribers to prevent data collection in those circumstances would be nonsensical. Further, Verizon Wireless’ privacy policy expressly provides for opt-in consent in other circumstances

²⁷ EPIC Comments at 3-4.

²⁸ See *Self-Regulatory Principles for Online Behavioral Advertising*, <http://www.iab.net/media/file/ven-principles-07-01-09.pdf> (July 2009) at 12-14.

²⁹ EPIC Comments at 7.

³⁰ See <http://www22.verizon.com/about/privacy/policy/#info>. For example, the policy provides:

We collect information about your use of our products and services. Information such as call records, websites visited, wireless location, application and feature usage, network traffic data, service options you choose, mobile and device number, and other similar information may be used for billing purposes, to deliver and maintain products and services, or to help you with service-related issues or questions.

where warranted.³¹ EPIC's assertions concerning Verizon Wireless' policies thus flatly contravene its own acknowledgement that "context" is important.³²

CONCLUSION

For the foregoing reasons and those discussed in Verizon Wireless' comments, the record reflects broad support for a technology- and competitively-neutral privacy framework applicable to all players, instead of additional regulation of service providers. Proponents of new regulation have provided no legal or factual basis for such an approach. Consumers' privacy needs and expectations in today's complex Internet environment should instead be addressed through venues such as NTIA's multi-stakeholder process.

Respectfully submitted,

/s/ Robert G. Morse

Michael E. Glover
Of Counsel

John T. Scott, III
Robert G. Morse
1300 I Street, N.W.
Suite 400 West
Washington, DC 20005
(202) 515-2400

Attorneys for Verizon Wireless

July 30, 2012

³¹ For example, the policy provides that "If Verizon intends to gather information from your use of our Internet access services to direct customized advertising specifically to you based on your visits over time and across different non-Verizon websites, we will provide you with notice of our plan and obtain your affirmative consent." *See id.*

³² *See* EPIC Comments at 10-11.